Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 23 mars 2006
N° CERTA-2006-AVI-125

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dana la mise en œuvre IPsec de FreeBSD

Gestion du document

Référence	CERTA-2006-AVI-125
Titre	Vulnérabilité dana la mise en œuvre IPsec de FreeBSD
Date de la première version	23 mars 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD du 22 mars 2006
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Contournement de la politique de sécurité.

2 Systèmes affectés

- FreeBSD 4.10 ;
- FreeBSD 4.11 ;
- FreeBSD 5.3 ;
- FreeBSD 5.4 ;
- FreeBSD 6.0.

3 Résumé

Une vulnérabilité dans la mise en œuvre du protocole `IPsec` sous `FreeBSD` permet à un utilisateur distant mal intentionné de contourner la politique de sécurité.

4 Description

`IPsec` est un protocole destiné a transporter des données chiffrées sur un réseau IP.

Le protocole `IPsec` met en œuvre un service anti-rejeu (`anti-replay service`), destiné à empêcher un utilisateur distant mal intentionné de rejouer des paquets.

Une vulnérabilité dans la mise en œuvre `fast_ipsec`, dans le service `anti-replay`, permet à un utilisateur mal intentionné de rejouer des paquets. Cette vulnérabilité est causée par une mauvaise vérification des numéros de séquence utilisés lors d'une connexion.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité FreeBSD SA-06-11 du 22 mars 2006 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06-11.ipsec.asc
- Référence CVE CAN-2006-0905 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0905

Gestion détaillée du document

23 mars 2006 version initiale.